MergePoint® 53xx Service Processor Manager Firmware Release Notes

V 1.4.0.11
October 22, 2009

This document includes:

1. Instructions for upgrading
2. Features and enhancements
3. Supported Service Processors (SP) and DirectCommand functionality per SP
4. Constraints and conditions
5. Features and enhancements from previous release 1.2.1.16

==========

1. Instructions for upgrading

==========

Please refer to the MergePoint appliance Installer/User Guide for more information on how to upgrade the MergePoint service processor manager to version 1.4.0.11.

NOTE: If the current version of the MergePoint SPM 5324/5340 is 1.2.0.13 or earlier, please upgrade to version 1.2.1.07 before upgrading to version 1.4.0.11.

This note does not affect the MergePoint SPM 5300 appliance.

==========

2. Features and enhancements

==========

The following features are added or bugs are fixed in this release:

1. Added support for Dell M1000e Chassis

NOTE: If the DSView® 3 management software is used with the MergePoint service processor manager for this feature, the DSView 3 software must be upgraded to version 3.7.1.58 to support this functionality. Specific CMC firmware versions used in M1000e compatibility testing include 1.30 and 2.00.

2. Added support for Dell iDRAC Blade Servers within M1000e Chassis

NOTE: If the DSView® 3 management software is used with the MergePoint service processor manager for this feature, the DSView 3 software must be upgraded to 3.7.1.58 to support this functionality.

Specific iDRAC or iDRAC6 blade servers/firmware versions used in compatibility testing include:

Blade Server	iDRAC Firmware Versions
PowerEdge M600 (iDRAC)	1.20 (Build 11) 1.40 (Build 12)
PowerEdge M605 (iDRAC)	1.1
PowerEdge M610 (iDRAC6)	2.02 (Build 4)
PowerEdge M710 (iDRAC6)	2.02 (Build 4)
PowerEdge M805 (iDRAC)	1.40 (Build 12)

3. Serial Over LAN Improvements

Serial Over Lan (SoL) behavior after reboot was improved to enable continued communications.

4. Stability Improvements

An issue that caused system instability and eventual shutdown when user profiles were added has been corrected.

5. Handling of Oversized Network Frames

An issue was corrected where the appliance would “lock up” when the MTU was configured to be greater than 1522 bytes and a frame larger than the MTU size was received.

Support Issues addressed in this release:

65542537 65555134 65529220 65528800

==========

3. Supported Service Processors (SP) and DirectCommand functionality per SP

==========

The following SPs are supported in this release. Note that we have not verified every SP model and firmware version, so some incompatibilities with particular models may be seen.

Service Processor	Notes
IPMI 1.5	
IPMI 2.0	
IBM® RSA II	Tested 3950 with firmware version A3EP36B.
IBM BladeCenter®	The BladeCenter Management Module (BCMM) is not supported, but its successor the Advanced Management Module (BCAMM) is supported. Tested with firmware version BPET48N.
DELL® DRAC 3	
DELL DRAC 4	

Service Processor	Notes
DELL DRAC 5	Tested PowerEdge 2950 with DRAC5 firmware version 1.33.
DELL 10G	Tested R805v running firmware version 1.44.
DELL BladeCenter DRAC/MC	Tested with firmware version 1.3 (build 06.12).
DELL M1000e Chassis	Tested with CMC firmware versions 1.30 and 2.00.
DELL iDRAC Blade Server: M600	Tested with iDRAC firmware versions 1.20 (Build 11), 1.40 (Build 12)
DELL iDRAC Blade Server: M605	Tested with iDRAC firmware version 1.1
DELL iDRAC Blade Server: M610	Tested with iDRAC firmware version 2.02 (Build 4)
DELL iDRAC Blade Server: M710	Tested with iDRAC firmware version 2.02 (Build 4)
DELL iDRAC Blade Server: M805	Tested with iDRAC firmware version 1.40 (Build 12)
HP® IPMI	Tested DL140 with IPMI 2.0 firmware version 2.12.
HP iLo	Tested DL585 with iLo firmware version 1.84.
HP iLo2	Tested DL385G2 with iLo2 firmware version 1.42.
HP BladeSystem	Tested with OA firmware version 1.30 and iLo2 blade firmware version 1.22.
SUN® iLom	Standalone SUN servers only. Blade servers not supported in this release.
SUN Alom	Standalone SUN servers only. Blade servers not supported in this release. Tested Fire Netra 240 with aLom firmware version 1.6.9.
Fujitsu Technology Solutions iRMC	Tested BX600S2 with iRMC firmware version 2.21G.
Fujitsu Technology Solutions iRMC S2	Tested RX200 S4 with iRMC2 firmware version 3.44A.
Sun eLOM	Tested Fire x2200 M2 with eLOM firmware version 3.20.

DirectCommand Functionality (Browser session / Auto login / vKVM) support per SP:

SP Type	Browser Session	Autologin	KVM	VM	KVM/VM Integrated	Specific Notes
IPMI1.5	Yes					1
IPMI2.0	Yes					1
ALOM	Yes					1
DRAC 3	Yes	Yes	Yes			2

SP Type	Browser Session	Autologin	KVM	VM	KVM/VM Integrated	Specific Notes
DRAC 4	Yes	Yes	Yes			3
DRAC 5	Yes	Yes	Yes			3, 4, 5
ILO	Yes	Yes	Yes	Yes		
ILO2	Yes	Yes	Yes	Yes (IE)	Yes (IE)	6
ELOM	Yes	Yes	Yes	Yes	Yes	7
IBM RSAII/SLIM	Yes	Yes	Yes	Yes	Yes	8, 9, 10, 11, 12
iRMC	Yes	Yes	Yes	Yes	Yes	
iRMC S2	Yes	Yes	Yes	Yes	Yes	
IBM BladeCenter	Yes	Yes	Yes	Yes	Yes	**Error! Reference source not found.**, 13, 28
IBM Blade			Yes*	Yes*		13
DRAC/MC	Yes*					15, 16
DRAC/MC Blade			Yes*	Yes*		15
HP BladeSystem	Yes*	Yes*				17
HP Blade			Yes*	Yes*		17
ILOM	Yes	Yes	Yes	Yes	Yes	18
M1000e	Yes	Yes				19, 20, 21, 22, 23
iDRAC Blades	Yes	Yes	Yes	Yes	Yes	22, 23, 24, 24, 26, 27

Specific Notes:

1. IPMI1.5, IPMI2.0 or ALOM has no web management interface itself by default, but it can be integrated with a web interface. In this case, when you customize a SP profile for the IPMI SP and set the web port and web scheme, you are able to use “Browser session”.
2. For web browsers in some particular OS (i.e. Linux), if Java Applet in the web browser have no privilege to listen on Port 443 of local IP address (127.*.*.*), the Browser session, autologin or vKVM won’t work. It is because the Java Applet in web page of Dell DRAC3 uses the hard-coded port 443 to communicate, but DirectCommand applets of MergePoint appliance can’t redirect the communication between the web client and DRAC3 via port 443 due to the privileges.
3. When the maximum number of sessions in DRAC4 or DRAC5 has been reached, the autologin or KVM will be failed. You need to reset the firmware of the SP via Telnet or SSH.
   The command for reset the SP firmware:
   racadm racreset

4. If DirectCommand launches for DRAC5 servers are unsuccessful, insure that the JRE is set to allow temporary file storage and that previous temporary files are deleted through the Java Control Panel.
5. Sometimes, vKVM DirectCommand launches for DRAC5 servers are unsuccessful and only show a blank screen when running from the Firefox browser. In this case, we have seen successful operation using the IE browser.
6. The iLO2 KVM runs with ActiveX in IE browser and with Applet in other browser (e.g. Firefox). The KVM with ActiveX integrates Virtual Media, while KVM with applet does not. iLO remote console (vKVM) does not support multi-session in MS IE via DirectCommand.
7. vKVM operation to ELOM servers may conflict with other network services commonly run on server machines. If conflicts occur, we suggest performing these operations on a workstation computer instead of a server computer.
8. When a vKVM session is connected on a RSA_II server, a second login with the same userid will cause the original vKVM session to be disconnected. So, a second login through the MergePoint SP manager will cause the first vKVM session to be disconnected. This behavior is by design in the RSA_II servers.
9. Intermittent load failures of the vKVM and VM applets on RSA_II servers are seen when the JRE is allowed to keep temporary files on the computer. When using these vKVM and VM applications on RSA_II servers, we recommend setting the JRE to disallow temporary file storage through the Java Control Panel.
10. vKVM operation to RSA_II servers launched through a browser login session may not be successful. We recommend using the vKVM autologin operation.
11. vKVM operation to RSA_II servers is incompatible with JRE-6u13. We recommend using JRE-6u11 or JRE-6u14 for these applications.
12. When managing RSA_II servers through the MergePoint SP manager while using DSView 3 software, DirectCommand sessions sometimes cannot be successfully launched when using JRE versions above 6u7 without disabling “the next-generation Java Plug-in” setting through the Java Control Panel. If these issues continue to occur disabling “the next-generation Java Plug-in”, we recommend downgrading the JRE to 6u7.
13. The Merge Chassis operation of IBM BladeChassis with the DSR® KVM over IP switch within the DSView 3 software fails to complete when the BladeChassis and blades are all discovered within the MergePoint SP manager. To workaround this issue, we recommend that the BladeChassis and DSR switch are discovered and merged within DSView software and the BladeChassis is discovered within the MergePoint SP manager, then each blade in the MergePoint SP manager-discovered chassis is individually merged with the associated blade in the DSView software-discovered chassis.
14. The KVM and vMedia function of IBM Blade is integrated with the KVM/vMedia of IBM BladeCenter’s KVM/vMedia. So you can access each blade through KVM applet of BladeCenter.
15. You can visit DRAC/MC’s digital KVM/vMedia for a blade through “Browser session” ONLY IF the client can communicate with the digital KVM’s IP directly.
16. Sometimes, autologin operation to DRAC-MC servers do not complete and display “Internet Explorer cannot display the webpage” (or blank page if default browser is FF3). The autologin operation has been observed to complete if the page is refreshed.
17. You can visit KVM/vMedia of a HP Blade through HP BladeCenter’s “Browser session” or “Autologin” interface ONLY IF the client can communicate with the Blade’s IP directly. HP Blade can’t be accessed directly from HP OA via DirectCommand. So if you want to visit the HP Blade via BladeCenter, you need to add every blade as an SP, and then you are able to visit the SP’s vKVM.
18. ILOM’s KVM/VM applet needs input username and password manually.
19. The M1000e web interface cannot be opened using the FireFox 3 browser, which also affects the browser link within the MergePoint appliance. Instead, the autologin link can be used, or Internet Explorer 7.
20. M1000e autologin sessions are not automatically restarted upon session timeout. Click the autologin link again to restart the session.
21. The M1000e "Single Sign-in" functionality cannot be supported when logged in using the browser login. Use autologin for this functionality.

22. When connecting to an iDRAC blade using the M1000e "Single Sign-in" feature, the blade's vKVM connection is only functional if the default vKVM ports are configured in the blade. If the vKVM ports are redefined, then vKVM is only supported through a DirectCommand *FIX GLOBALLY session to the blade.
23. The CMC web interface login selection within the iDRAC blade web interface is not forwarded through the MergePoint appliance. Instead, the M1000e autologin link should be used to access the CMC web interface.
24. Occasionally, autologins to an iDRAC blade are rejected, and a DirectCommand Applet Error is presented that contains an error string from the blade such as "Failure_Session_Creation". Workarounds include retrying the autologin after a few minutes, retrying blade login through the chassis Single Sign-in feature, or resetting the blade.
25. Sometimes after a session expires, the iDRAC blade logout selection is not processed. If this occurs, close the browser window or tab.
26. The autologin associated with an iDRAC blade vKVM session is not automatically terminated and must be allowed to time out.
27. Some anomalies have been seen with the Dell M610 blade when it is either directly managed or managed through the MergePoint appliance. These anomalies include:
    a. The default root/calvin uid/password does not always allow access, yet another defined user name does seem to work.
    b. Virtual Media does not connect.

    Please check the Dell web site for release note updates.
28. A DirectCommand vKVM session on an IBM BladeCenter running BPET48N firmware will unexpectedly terminate after two minutes. A vKVM session launched from a DirectCommand manual login does not exhibit this issue.

General Notes:

1. Browser session functionality is implemented as pure port forwarding. The web interfaces of some SPs may work abnormally in this mode regardless of the port forwarding implementation. Sometimes, DirectCommand session options are not presented after enabling DirectCommand through the OBWI when running Firefox 3.5. If this occurs, we recommend downgrade to Firefox 3.0.11.
2. If login prompts are presented during autologin DirectCommand sessions, the login username/password associated with that SP stored within the MergePoint SP manager may need to be reentered.
3. Login process for the M1000e may take up to 20 seconds after proper username and credentials are presented and therefore some impact to display information at the OBWI may be seen (e.g. Displaying power information may take 15 – 20 seconds for an M1000e chassis) when accessing various MergePoint SP manager features.
4. If DirectCommand launch fails with a "Unable to launch the application" message, please try either:
    a) Downgrading the Java version to JRE-1.6.0_11 or earlier
    b) Unchecking the "Enable the next-generation Java Plug-in" option in the Java control panel

==========

4. Constraints and Conditions

==========

This release includes the following constraints or conditions:

1. Usernames under User Configuration must be all in lowercase letters.

2. BMC Provisioning can only be configured on the secondary Ethernet Interface (eth1).
3. We support alias for every SP. Do not use special characters in the alias. Only the following characters are allowed: “0—9”, “a—z”, “A—Z” and “-“.
4. Power outage during the upgrading process is not recoverable.
5. Not allowed to use special characters in the SP’s password. We do not support the characters like >’, ‘<’, “‘”, “””,”&” or “|”.
6. **Configuration of a private subnet range within 192.168.0.1 to 192.168.0.255**
   Please note that the MergePoint SP manager reserves 192.168.0.10 and 192.168.0.20 as default addresses for eth0 and eth1 respectively. To configure a private subnet using this 192.168.0.x address range, the eth0 and eth1 addresses must be moved from this range. If IP address conflicts occur after reconfiguring, please contact Avocent Technical Support for a work instruction with more details.
7. A pre-configured hostname for a service processor, when delivered to the MergePoint appliance DHCP server, will be used as the default alias name. Otherwise, the IP address will be used as the default alias name.
8. With respect to the M1000e CMC chassis power down command, all servers within the chassis must power down successfully in order for the M1000e CMC to power down successfully. Otherwise, an error message is delivered to the OBWI indicating a protocol failure due to the M1000e chassis command not completing. This behavior is specific to the M1000e CMC and not to the MergePoint appliance OBWI.
9. Occasionally, a MergePoint appliance configured with a static IP address may revert to a dynamic IP address following a web upgrade. Please reboot the MergePoint appliance to restore the static IP address.
10. When using PXE provisioning and DHCP assigned addresses, both services should not be executing simultaneously. This action may cause the DHCP service to errantly assign an address for which the PXE provisioning service is responsible and vice versa.

==========

5. Features and enhancements from previous release 1.2.1.16

==========

This release adds further enhancements and bug fixes to the feature set originally released as version 1.2.0.7.

The following features are added or bugs are fixed in this release:

1. Improved RSA_II DirectCommand functionality

Corrected interoperability issues with autologin and vKVM operation where “SP unavailable” message was sometimes displayed and vKVM viewer applet did not initialize properly.

NOTE: If the DSView software is used with the MergePoint SP manager for this feature, the DSView software be upgraded to version 3.7.0.151 to support this functionality.

Specific RSA_II server/firmware compatibility verified in testing of this release includes:

Server	ASM Firmware Version
x3550	GFEP33B
x3650	GGEP36B
x3650	GGEP37A
x3950	A3EP36B

2. **Enhanced Alert messaging**
   Corrected issue where the “From” address on alert E-mails from the MergePoint SP manager did not include domain name.

Support Issues addressed in this release:

65537325	65530042	65523922	65426507	65529220 (partial)
65531248	65526554			

The following features are added or bugs are fixed in previous releases starting with version 1.2.0.7:

1. **Added system session status page**
   For each of managed service processor, there is System Session web page showing its session status.
2. **Connection test for DirectCommand**
   Connection test for DirectCommand tells user why the DirectCommand operation is failed. This feature saves the time and effort for troubleshooting of this problem.
3. **Supported setup wizard for deployment**
   Setup wizard tells user where to start. This lets user spend less time on configuration and deployment. The wizard configuration can also be saved to a file and applied to another appliance.
4. **Supported default IP address**
   If MergePoint appliance is failed to obtain an IP address from DHCP server, the default IP address will be used instead.
5. **Supported new service processor: Sun eLOM**
6. **Supported new service processor: Fujitsu Technology Solutions iRMC S2**
7. **Improved license page**
   Improved license web page shows not only how many licenses are used, but also how many licenses are available.
8. **Solved the problem of abnormal exiting of SoL session**
   Fixed the problem of abnormal exiting of SoL session when user type ‘Ctrl+C’.
9. **Changed default root password from ‘avocent’ to ‘Sydney’**
10. **Changed menu system for console application for MergePoint 5200 appliance and MergePoint 5300 appliance**
11. **Supported the distinguishing between DELL DRAC3 and DELL DRAC4 in Discovery**
12. **Supported the distinguishing between HP iLO and HP iLO2 in Discovery**
13. **Added support for Sun iLOM in Discovery**
    Discovery can show iLOM as its real type. The previous versions of Discovery can only show it as IPMI.
14. **Fixed the bug of “Cannot start DHCP service when Domain Name is empty.”**
15. **Fixed the bug of Discovery and Manage DELL DRAC3 ERA (Embedded RAC Access Controller)**
16. **Added safe shutdown for the appliance, and enhanced file system**
    Added safe shutdown function in the appliance. User can safely power off the appliance with it. In addition, Ext3 is used instead of Ext2. If the file system of the appliance is corrupt, it will try to fix the file system first. If it is not recoverable, then the appliance will run with factory default settings.

17. **Improved the performance of DirectCommand**
    The time used to setup a DirectCommand is decreased. It's faster to connect DirectCommand.
18. **Showed actual DSView software user in the active session for sessions created from the DSView software Supported SuperMicro IPMI 2.0 card.**
19. **Recorded accounting Logs for both starting and stopping system sessions.**
20. **Support to show HP iLo/iLo2 IML (iLo Management Log).**
21. **Fixed compact flash corruption issues.**
    Disabled unnecessary writes and corrected a control register offset.